JOURNAL OF ALGEBRA 81, 72–99 (1983)

Quotient-Singularities and Wild p-Cyclic Actions

BARBARA R. PESKIN*

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801

Communicated by D. Buchsbaum

Received August 13, 1981

In this paper we develop canonical forms for certain p-cyclic automorphisms of formal power series rings over fields of characteristic p. Our interest in this problem is based on the geometrical question of classifying quotient-singularities over fields of non-zero characteristic.

Let V be a smooth variety over an algebraically closed field k of arbitrary characteristic. Given a finite group G of k-automorphisms of V, we can consider the quotient-variety V/G, whose points correspond to orbits of points in V. The variety V/G is smooth almost everywhere, but may acquire singularities corresponding to points of V with non-trivial isotropy. One would like to classify all singularities which can arise in this manner.

In characteristic zero, this problem has been extensively studied and a complete classification has been given by Brieskorn [4] in the case that V has dimension two. The key to the characteristic zero solution is a result of Cartan [5] which states that it is possible to choose coordinates for V so that G acts linearly. Thus the study reduces to a classification of quotients by matrix group actions. This reduction has the twofold advantage of greatly restricting the classes of actions to be analyzed as well as of bringing the action into a form for which explicit calculations are particularly straightforward.

However, in non-zero characteristics this method breaks down: if the characteristic divides the order of G—the case of wild actions—it is rarely possible to linearize the action of the group. Consequently, very little progress has been made in the study of characteristic p quotients except in certain restricted cases in which G acts linearly (see, for example, [8]).

The purpose of this work is to construct normal forms for non-linear wild group actions and use them to study the resulting quotient-singularities. We concentrate on the case that G is cyclic of order p.

* Current address: Department of Mathematics, Mount Holyoke College, South Hadley, MA 01075.

0021-8693/83 $3.00

After reviewing the necessary facts from commutative algebra in Section 1, we begin our analysis of p-cyclic automorphisms by developing a partial linearization for the action of G. A program is then established for studying these actions in the case that G is generated by an element whose linear part consists of a single Jordan block. The remainder of the paper is devoted to applying this method to the study of actions in dimensions 2 and $p-1$.

1. Preliminaries

Let R be a normal noetherian local k-algebra of dimension n over an algebraically closed field k. Given a finite group G of k-automorphisms of R, we denote by R^G the ring of invariants of R under the group action. If $V = \operatorname{Spec} R$, then the quotient-space of V with respect to the induced G-action is defined by $V/G = \operatorname{Spec} R^G$. We first observe

PROPOSITION 1.1. *The ring R^G is a normal n-dimensional local ring.*

Geometrically, the inclusion $R^G \to R$ corresponds to the covering map $\pi: V \to V/G$, which has degree equal to the order of G. If R is regular, then V is smooth and the quotient-space V/G is smooth wherever the map π is unramified. The image of the ramification locus may, however, be singular in V/G.

PROPOSITION 1.2. *Let R be a regular noetherian normal ring and let $\mathfrak{p} \subset R$ be a minimal prime of the ramification locus of the map $R^G \to R$. If* $\operatorname{ht} \mathfrak{p} \geqslant 2$, *then R^G is singular along the image of* $\mathfrak{p}$.

Proof. Let $\mathfrak{p}' = p \cap R^G$ and consider the localization $(R^G)_{\mathfrak{p}'} \to R_{\mathfrak{p}}$ of the map $R^G \to R$ at $\mathfrak{p}'$. Since $\mathfrak{p}$ is a minimal prime of the ramification locus, the localized map is unramified except above $\mathfrak{p}'$. It follows from the purity of the branch locus [14] that the ring $R^G_{\mathfrak{p}'}$ is singular because the ramification lies in codimension greater than one. Now $R_{\mathfrak{p}'}$ is a regular ring and so $R^G_{\mathfrak{p}'}$ is regular wherever the map is unramified. Therefore the singular locus lies entirely along the prime $\mathfrak{p}'$. ∎

Consequently, if the map $R^G \to R$ ramifies only at the maximal ideal of R, the quotient space V/G will have an isolated singularity at its closed point, provided $n \geqslant 2$. We wish to examine which singularities can be obtained as such quotients of smooth spaces by analyzing the structure of the invariant rings R^G.

In studying fixed rings, there are two invariants which are particularly useful:

DEFINITION 1.3. Given any $x \in R$, the *norm* of x, denoted Nx, is defined to be

$$Nx = \prod_{\sigma \in G} \sigma x$$

and the *trace* of x, denoted $\operatorname{tr} x$, is

$$\operatorname{tr} x = \sum_{\sigma \in G} \sigma x.$$

Clearly both Nx and $\operatorname{tr} x$ are elements of R^G and so norm and trace determine mappings from R to R^G. If the order of G, call it g, is prime to the characteristic of k, then the modified trace map

$$\frac{1}{g} \operatorname{tr}: R \to R^G$$

defines an R^G-module homomorphism projecting R onto R^G. This map is fundamental in the analysis of characteristic zero quotients. For example, it allows one to prove that depth $R^G \geqslant$ depth R and hence that singularities arising as quotients of smooth varieties are always Cohen–Macaulay (see [7]).

However, if the characteristic divides the order of G, the trace map degenerates and with it the Cohen–Macaulay property of quotient-singularities. Fogarty [7] has shown

PROPOSITION 1.4. *Let $d = 0, 1,$ or 2. If* depth $R \geqslant d$, *then* depth $R^G \geqslant d$.

However, he has demonstrated strong upper bounds on the depth:

PROPOSITION 1.5. *Let* char $k = p$ *and let G be a cyclic group of order p^v acting on a normal noetherian local k-algebra R. Assume that the induced action of G on* Spec R *is free except at the closed point. If* depth $R \geqslant 2$, *then* depth $R^G \leqslant 2$.

Combining these propositions, we obtain

COROLLARY 1.6. *Let* char $k = p$ *and let R be a regular noetherian local k-algebra of dimension $\geqslant 2$. If G is a cyclic group of order p^v such that $R^G \to R$ ramifies only at the maximal ideal of R, then* depth $R^G = 2$.

Consequently, isolated quotient-singularities arising from wild group actions are rarely Cohen–Macaulay in dimensions greater than two.

We develop a slightly more general formulation of Proposition 1.5, which will be needed later.

LEMMA 1.7. *If R is a noetherian local ring and $\mathfrak{p}$ is a prime ideal of R, then* depth $R \leqslant \operatorname{depth}(R_\mathfrak{p}) + \dim(R/\mathfrak{p})$.

Proof. If depth $R = 0$, the lemma is clear. Assume that depth $R \geqslant 1$ and that there is some $r \in \mathfrak{p}$ which is not a zero-divisor in R. Then r is not a zero-divisor in $R_\mathfrak{p}$ and, setting $R' = R/(r)$, we have depth $R' =$ depth $R - 1$, depth $R'_\mathfrak{p} =$ depth $R_\mathfrak{p} - 1$ and $R/\mathfrak{p} = R'/\mathfrak{p} \cap R'$ since $r \in \mathfrak{p}$. Proceed by induction.

If $\mathfrak{p}$ contains no R-regular elements, then there is a prime $\mathfrak{q} \in \operatorname{Ass}(R)$ which contains $\mathfrak{p}$. But depth $R \leqslant \dim(R/\mathfrak{q})$ for all $\mathfrak{q} \in \operatorname{Ass}(R)$ [10, VI, Theorem 27] and $\dim(R/\mathfrak{q}) \leqslant \dim(R/\mathfrak{p})$ since $\mathfrak{p} \subset \mathfrak{q}$. ∎

PROPOSITION 1.8. *Let* char $k = p$ *and let R be a normal noetherian local k-algebra. Let G be a group of k-automorphisms of R, cyclic of order p^r, and assume that the map $R^G \to R$ is ramified only along the prime $\mathfrak{p} \subset R$. Then* depth $R^G \leqslant 2 + \dim(R/\mathfrak{p})$.

Proof. Let $\mathfrak{p}'$ denote the restriction of $\mathfrak{p}$ to R^G and consider the map $(R^G)_\mathfrak{p} \to R_{\mathfrak{p}'}$. Note that $(R^G)_{\mathfrak{p}'} = (R_{\mathfrak{p}'})^G$ and that the localized map is ramified only at the maximal ideal. If $\operatorname{ht} \mathfrak{p}' < 2$, then $\operatorname{depth}(R^G)_{\mathfrak{p}'} \leqslant \dim(R^G)_{\mathfrak{p}'} < 2$. If $\operatorname{ht} \mathfrak{p}' \geqslant 2$, then $\operatorname{depth}(R_{\mathfrak{p}'}) \geqslant 2$ by Serre's criterion for normality. Therefore $\operatorname{depth}(R^G)_{\mathfrak{p}'} \leqslant 2$ by Proposition 1.5. Also $\dim(R^G/\mathfrak{p}') = \dim(R/\mathfrak{p})$ by the theorems of Cohen–Seidenberg since the map $R^G \to R$ is finite. Applying Lemma 1.7, we conclude

$$\begin{aligned} \operatorname{depth} R^G &\leqslant \operatorname{depth}(R^G)_{\mathfrak{p}'} + \dim(R^G/\mathfrak{p}') \\ &\leqslant 2 + \dim(R/\mathfrak{p}). \quad ∎ \end{aligned}$$

Remark 1.9. Ellingsrud and Skjelbred [6] have shown that the inequality in Proposition 1.8 can be strengthened to equality in the case that R is a polynomial ring, the action of G is linear and the map $R^G \to R$ is totally ramified along $\mathfrak{p}$. Note that equality also holds for a formal power series ring R with linear action since depth is preserved under passage to the completion.

2. A PARTIAL LINEARIZATION

In this section we develop a standard form for nonlinear group actions and set up a program for analyzing these actions by means of linear models. Because we are interested only in the local behavior of the quotient-space near its singular points, we will work with complete local rings. Therefore let

$R = k[[u_1,..., u_n]]$ be the ring of formal power series in n letters over an algebraically closed field k of characteristic p and let G be a finite group of k-automorphisms of R.

PROPOSITION 2.1. *If the order of G is divisible by p and the map $R^G \to R$ ramifies only at the maximal ideal $\mathfrak{m} \subset R$, then it is not possible to choose coordinates for R so that G acts linearly.*

Proof. Assume that coordinates u_i could be found. Since the order of G is p-divisible, there is an element $\sigma \in G$ which has order p. We may assume that the coordinates u_i have been chosen so that σ is in Jordan form. Because $\sigma^p = 1$, every eigenvalue of σ is a pth root of unity: in characteristic p this forces every eigenvalue to be 1. Therefore σ has the form

$$\begin{aligned}
\sigma u_1 &= u_1, \\
\sigma u_2 &= u_2 + \varepsilon_1 u_1, \\
&\vdots \\
\sigma u_n &= u_n + \varepsilon_{n-1} u_{n-1},
\end{aligned}$$

where, for each i, the number ε_i is either 0 or 1. But this action fixes the one-dimensional locus $\{u_1 = \cdots = u_{n-1} = 0\}$, i.e., the u_n-axis, which contradicts the assumption that $R^G \to R$ ramifies only at $\mathfrak{m}$. ∎

Therefore, unlike in characteristic zero, wild group actions cannot, in general, be brought into linear form and so it is necessary to develop new normal forms for these inhomogeneous actions. We restrict our attention to the case that G is cyclic of order p.

Let σ be a generator of G. The action of σ can be realized as a system of n power series in $u_1,..., u_n$, one for the image of each u_i under σ. Such a system defines an automorphism of R provided the linear terms of the power series define an invertible linear transformation. Therefore σ has the form

$$\begin{aligned}
\sigma u_1 &= a_{11} u_1 + a_{12} u_2 + \cdots + a_{1n} u_n + h_1(u_1,..., u_n), \\
&\vdots \\
\sigma u_n &= a_{n1} u_1 + a_{n2} u_2 + \cdots + a_{nn} u_n + h_n(u_1,..., u_n),
\end{aligned}$$

where $a_{ij} \in k$ are such that $\det |a_{ij}| \neq 0$ and $h_i \in R$ has order $\geqslant 2$.

Denote by $\bar{\sigma}$ the invertible transformation determined by the linear terms of σ, i.e., the matrix action given by (a_{ij}). By a suitable change of coordinates we may assume that $\bar{\sigma}$ is in Jordan form and, as in the proof of the proposition, all eigenvalues of $\bar{\sigma}$ are 1. The matrix representing $\bar{\sigma}$ is therefore composed of blocks of the form

$$\begin{pmatrix} 1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 1 \end{pmatrix}.$$

LEMMA 2.2. *The maximal size of a Jordan block of $\bar{\sigma}$ is p.*

Proof. The automorphism σ, and hence its linear part $\bar{\sigma}$, has order p. Therefore $\bar{\sigma} - 1$ is nilpotent of index p, for

$$(\bar{\sigma} - 1)^p = \bar{\sigma}^p - 1 = 0.$$

It follows that no Jordan block of $\bar{\sigma}$ can have dimension greater than p. ∎

The action of σ itself is therefore defined by blocks of the form

$$\begin{aligned} \sigma u_i \quad &= u_i + h_i(u_1, ..., u_n), \\ \sigma u_{i+1} &= u_{i+1} + u_i + h_{i+1}(u_1, ..., u_n), \\ &\vdots \\ \sigma u_{i+j} &= u_{i+j} + u_{i+j-1} + h_{i+j}(u_1, ..., u_n), \end{aligned} \tag{2.3}$$

where $h_l \in R$ has order $\geqslant 2$ and the block size $(= j + 1)$ is at most p. Although it is not possible, in general, to eliminate all of the higher-order contributions h_l, it is always possible to partially linearize the action:

THEOREM 2.4. *Let $R = k[[u_1, ..., u_n]]$ and let σ be a k-automorphism of R of order p. Then there exists a choice of coordinates for R so that σ is composed of blocks of the form*

$$\begin{aligned} \sigma u_i \quad &= u_i + f_i(u_1, ..., u_n), \\ \sigma u_{i+1} &= u_{i+1} + u_i, \\ &\vdots \\ \sigma u_{i+j} &= u_{i+j} + u_{i+j-1}, \end{aligned} \tag{2.5}$$

where $f_i \in R$ has order $\geqslant 2$ and the block size, $j + 1$, is at most p. If $j + 1 = p$, then $f_i = 0$ and the action within the block is linear. If $R^G \to R$ ramifies only at the maximal ideal $\mathfrak{m} \subset R$, then $j + 1 < p$ and $f_i \neq 0$.

Proof. We may assume that σ is composed of blocks of the form (2.3). Within each block, choose new coordinates $\bar{u}_l$ as follows:

Let

$$\begin{aligned}
\bar{u}_{i+j} &= u_{i+j},\\
\bar{u}_{i+j-1} &= (\sigma-1)\,u_{i+j} = u_{i+j-1} + h_{i+j},\\
\bar{u}_{i+j-2} &= (\sigma-1)^2 u_{i+j} = u_{i+j-2} + h_{i+j-1} + (\sigma-1)\,h_{i+j},\\
&\vdots\\
\bar{u}_i &= (\sigma-1)^j u_{i+j} = u_i + h_{i+1} + (\sigma-1)\,h_{i+2} + \cdots + (\sigma-1)^{j-1} h_{i+j}.
\end{aligned} \tag{2.6}$$

Note that the Jacobian of the map $u_l \mapsto \bar{u}_l$ at $(0,..., 0)$ is the identity matrix, so the $\bar{u}_l$'s define a coordinate system for R. Setting

$$f_i = (\sigma-1)\,\bar{u}_i = h_i + (\sigma-1)\,h_{i+1} + \cdots + (\sigma-1)^j h_{i+j},$$

we have

$$\sigma\bar{u}_{i+l} = \bar{u}_{i+l} + \bar{u}_{i+l-1} \qquad \text{for } 0 < l \leqslant j$$

and

$$\sigma\bar{u}_i = \bar{u}_i + f_i.$$

Thus σ has the required form.

By Lemma 2.2, no block of σ can have dimension greater than p. If the dimension equals p, then $\bar{u}_i = (\sigma-1)^j u_{i+j} = (\sigma-1)^{p-1} u_{i+j}$. Consequently,

$$f_i = (\sigma-1)\,\bar{u}_i = (\sigma-1)^p u_{i+j} = (\sigma^p - 1)\,u_{i+j} = 0,$$

and so the action is linear. Note that this forces the element $\bar{u}_i$ to be fixed.

If $R^G \to R$ ramifies only at $\mathfrak{m}$, no element $\bar{u}_l$ can be invariant. This implies $f_i \neq 0$ and hence that the block size is strictly less than p. ∎

The theorem shows that all the nonlinear contributions in σ can be pushed to the top of each Jordan block, leaving the remainder of the action in linear form.

Now suppose that the action of σ is not linear, i.e., at least one $f_i \neq 0$. In this case, the process of forming successively higher powers of $(\sigma-1)^l u_{i+j}$ used in defining the new coordinate system (2.6) can be continued within each block until the result is zero. With notation as in (2.5), set

$$\begin{aligned}
f_i^1 &= f_i = (\sigma-1)^{j+1} u_{i+j},\\
f_i^2 &= (\sigma-1)^{j+2} u_{i+j},\\
&\vdots\\
f_i^l &= (\sigma-1)^{j+l} u_{i+j}.
\end{aligned}$$

Since $(\sigma - 1)^p = 0$, the element f_i^{p-j} is zero, but it is possible that $f_i^l = 0$ for $l < p - j$. Let m be the last index for which $f_i^m \neq 0$. Then *the extended form* for the action of σ within the block (2.5) is given by

$$\begin{aligned}
\sigma f_i^m &= f_i^m, \\
\sigma f_i^{m-1} &= f_i^{m-1} + f_i^m, \\
&\vdots \\
\sigma f_i^1 &= f_i^1 + f_i^2, \\
\sigma u_i &= u_i + f_i^1, \\
&\vdots \\
\sigma u_{i+j} &= u_{i+j} + u_{i+j-1},
\end{aligned} \tag{2.7}$$

where $f_i^l \in R$ has order $\geqslant 2$. If the action is similarly extended within each Jordan block, we obtain a set of power series $\{f_i^j\}_{i,j}$ in $u_1, ..., u_n$.

Now consider the power series ring $S = k[[u_1, ..., u_n; ..., w_i^j, ...]]$, where one variable w_i^j is added for each power series f_i^j occurring in the extended form for σ. The ring S has a natural linear action defined by letting σ act as in (2.7) with the new variables w_i^j replacing the f_i^j. Moreover, the ring R with its nonlinear action can be obtained from S by the map $\psi\colon S \to R$ defined by

$$\begin{aligned}
\psi(u_i) &= u_i, \\
\psi(w_i^j) &= f_i^j(u_1, ..., u_n),
\end{aligned}$$

which is compatible with the group actions. The map ψ thus exhibits R as a nonlinear slice of S.

Rather than compute the invariants of the inhomogeneous action of σ on R, we instead study the invariants for the ring S. Because σ acts homogeneously on S, the invariant ring S^G is often easier to understand than R^G despite its increased dimension. It then remains to study how information from S^G passes to information on R^G.

3. The Method of Nonlinear Slicing

We illustrate the method outlined above by studying the most basic case—that in which σ has only one Jordan block and the element f_i^1 is fixed so that there is only one power series f_i^j in the extended action (2.7).

Assume, then, that σ is a p-cyclic automorphism of R defined by

$$\begin{aligned} \sigma u_1 &= u_1 + f, \\ \sigma u_2 &= u_2 + u_1, \\ &\vdots \\ \sigma u_n &= u_n + u_{n-1}, \end{aligned} \tag{3.1}$$

where $f \in R$ has order $\geqslant 2$ and is invariant under σ. By Theorem 2.4, the dimension n of the ring R is at most p. If $n = p$, the element f is zero and the action is linear. Since we wish to study possible forms for non-linear actions, we will assume $n \leqslant p - 1$. On the other hand, if $n = 1$ the invariant ring R^G is normal and one-dimensional, hence regular, and so the quotient-space is smooth. We therefore restrict our attention to the range $2 \leqslant n \leqslant p - 1$.

The invariant ring R^G is a complete n-dimensional ring whose structure varies with the ramification locus of the map $R^G \to R$.

LEMMA 3.2. *Let G be any group of automorphisms of R which is cyclic of prime order. Let σ be a generator of G. Then the map $R^G \to R$ ramifies only at the maximal ideal $\mathfrak{m} \subset R$ if and only if the ideal $\mathfrak{r} = (\sigma u_1 - u_1, \ldots, \sigma u_n - u_n)$ is $\mathfrak{m}$-primary.*

Proof. The map $R^G \to R$ is ramified along the prime $\mathfrak{p}$ if and only if $\mathfrak{p}$ is fixed by σ and the induced action of σ on $R/\mathfrak{p}$ is trivial.

Assume that the map ramifies along a non-maximal prime $\mathfrak{p}$. The action on $R/\mathfrak{p}$ is then trivial and so $\sigma u_i - u_i \in \mathfrak{p}$ for all i. Therefore $\mathfrak{r} \subset \mathfrak{p}$ and hence is not $\mathfrak{m}$-primary.

Conversely, if $\mathfrak{r}$ is not $\mathfrak{m}$-primary, there is a non-maximal prime $\mathfrak{p}$ containing it. Therefore $\sigma u_i - u_i \in \mathfrak{p}$ for all i and so $\mathfrak{p}$ is fixed by σ and the action mod $\mathfrak{p}$ is trivial. Hence $R^G \to R$ ramifies along $\mathfrak{p}$. ∎

To study the ramification locus it therefore suffices to examine the primes associated to the ideal $\mathfrak{r} = (\sigma u_1 - u_1, \ldots, \sigma u_n - u_n)$. For the action (3.1) above, this ideal is equal to $(f, u_1, \ldots, u_{n-1})$ and so the structure of R^G splits into two cases determined by the choice of f.

PROPOSITION 3.3. *Let σ be the automorphism of R defined by* (3.1).

(i) *If f contains a term of the form u_n^i, then $R^G \to R$ ramifies only at* $\mathfrak{m}$ *and R^G has an isolated singularity.*

(ii) *If f contains no u_n^i term, then $R^G \to R$ ramifies along the dimension one prime $\mathfrak{q} = (u_1, \ldots, u_{n-1})$ and, if $n > 2$, the ring R^G is singular along the image of* $\mathfrak{q}$.

Proof. In the first case, the ideal $\mathfrak{r}$ is $\mathfrak{m}$-primary and the result follows from Lemma 3.2 and Proposition 1.2. In the second case, the ideal $\mathfrak{r}$ is equal to $(u_1,..., u_{n-1})$ and again the result follows from Proposition 1.2. ∎

Now consider the $(n+1)$-dimensional ring $S = k[[u_0, u_1,..., u_n]]$. The p-cyclic group G acts on S by letting σ act by

$$\begin{aligned} \sigma u_0 &= u_0, \\ \sigma u_1 &= u_1 + u_0, \\ &\vdots \\ \sigma u_n &= u_n + u_{n-1}. \end{aligned} \tag{3.4}$$

The resulting invariant ring S^G is a complete $(n+1)$-dimensional ring and the map $S^G \to S$, like the map $R^G \to R$, has degree p and ramifies only in low dimensions.

PROPOSITION 3.5. *The map $S^G \to S$ is ramified along the prime $\mathfrak{p} = (u_0, u_1,..., u_{n-1})$. Hence S^G is singular along the one-dimensional locus determined by $\mathfrak{p}' = \mathfrak{p} \cap S^G$.*

Proof. The ramification ideal $\mathfrak{r} = (\sigma u_0 - u_0,..., \sigma u_n - u_n)$ is equal to $(u_0, u_1,..., u_{n-1})$. The result now follows from Proposition 1.2 and the fact that $\dim S \geqslant 3$. ∎

The ring S maps to R by the homomorphism $\psi: S \to R$ defined by

$$\begin{aligned} \psi(u_0) &= f(u_1,..., u_n), \\ \psi(u_i) &= u_i \qquad \text{for } i \geqslant 1, \end{aligned} \tag{3.6}$$

which assigns to u_0 the invariant power series $f \in R^G$. Since ψ is compatible with the group actions on S and R, there is an induced map $\varphi: S^G \to R^G$ between the invariant subrings.

Now ψ, being a map between regular power series rings, is easily understood: it is surjective with kernel generated by $(u_0 - f)$. However, the map φ between the invariant subrings is far more complicated. For example, the element $(u_0 - f)$ lies in S^G only if $f = 0$ and so, for nonlinear automorphisms of R, it cannot generate the kernel of φ.

To derive results for φ analogous to those for ψ it is necessary to introduce an additional hypothesis on S^G.

DEFINITION 3.7. An integral domain R is *factorial* if every height 1 prime is principal.

The following criterion of Samuel [12] is useful for verifying the factoriality of invariant rings.

THEOREM 3.8. *Given a factorial ring R, let R^* denote the group of units in R. Let G be a cyclic group of automorphisms of R such that the map $R^G \to R$ is unramified in codimension one. Then the invariant ring R^G is factorial if and only if $H^1(G, R^*) = 0$.*

Using this criterion, Fossum and Griffith [8] have shown

THEOREM 3.9. *The ring S^G is factorial if $n = p - 1$.*

The analogous result for general n is not known and we state it as

Conjecture 3.10. The ring S^G is factorial for $2 \leqslant n < p - 1$.

Under the assumption that S^G is factorial we can analyze the kernel and image of the map φ.

PROPOSITION 3.11. *If the ring S^G is factorial, then there exists a unit $s \in S$ such that $(u_0 - f)\, s \in S^G$ and hence* $\ker \varphi = ((u_0 - f)\, s)\, S^G$.

Proof. Consider the image of $(u_0 - f)$ under σ:

$$\begin{aligned}\sigma(u_0 - f) &= u_0 - \sigma f \\ &= u_0 - f - (\sigma f - f).\end{aligned}$$

The element $\sigma f - f$ lies in $\ker \psi$ because f is invariant in R, and therefore it has the form $(u_0 - f)\, t$ for some $t \in S$. Consequently,

$$\begin{aligned}\sigma(u_0 - f) &= (u_0 - f) - (u_0 - f)\, t \\ &= (u_0 - f)(1 - t).\end{aligned}$$

Now $N(u_0 - f) = N(\sigma(u_0 - f)) = N(u_0 - f)\, N(1 - t)$, and hence $1 - t$ has norm 1. Since the ring S^G is factorial, Theorem 3.8 implies that the cohomology group $H^1(G, S^*)$ vanishes, where S^* is the group of units of S. Recall that

$$H^1(G, S^*) = \{\text{elements of } S^* \text{ with norm } 1\}/\{\text{image of } (\sigma/id)\, S^*\}.$$

Since $1 - t$ has norm 1, it is therefore possible to find a unit $s \in S^*$ such that $\sigma s/s = (1 - t)^{-1}$. For this choice of s,

$$\begin{aligned}\sigma((u_0 - f)\, s) &= (u_0 - f)(1 - t)\, \sigma s \\ &= (u_0 - f)(1 - t)(1 - t)^{-1} s \\ &= (u_0 - f)\, s.\end{aligned}$$

Thus the element $(u_0 - f)\, s$ lies in S^G.

Clearly $((u_0 - f)\, s)\, S^G \subset \ker \varphi$. The opposite inclusion follows from the fact that s is a unit: given any $x \in \ker \varphi$, there is an element $y \in S$ such that $x = (u_0 - f)\, y$. Then $x = (u_0 - f)\, s(s^{-1}y)$ and $s^{-1}y \in S^G$ because both x and $(u_0 - f)\, s$ are fixed by σ. ∎

It follows from this characterization of $\ker \varphi$ that the inverse image of any element $w \in \operatorname{Im} \varphi$ includes elements w' of the same order as w:

PROPOSITION 3.12. *Given any $w \in R^G$ which lies in the image of φ, there exists an element $w' \in S^G$ such that $\varphi(w') = w$ and* $\operatorname{ord} w' = \operatorname{ord} w$.

Proof. We first establish the proposition in the case $w = f$. Let s be given as in the preceding proposition. We may assume that the constant term of s is 1, so that s has the form

$$s = 1 + s_0 + h,$$

where $s_0, h \in S$ and s_0 consists of all terms of s having degrees 1 through $\operatorname{ord}(f) - 2$. Then

$$\begin{aligned}\sigma((u_0 - f)\, s) &= (u_0 - f)(1 + \sigma s_0 + \sigma h)\\ &= u_0 + u_0 \cdot \sigma s_0 + (\text{terms of degree} \geqslant \operatorname{ord} f).\end{aligned}$$

On the other hand, the element $(u_0 - f)\, s$ is invariant under σ and hence

$$\begin{aligned}\sigma((u_0 - f)\, s) &= (u_0 - f)(1 + s_0 + h)\\ &= u_0 + u_0 s_0 + (\text{terms of degree} \geqslant \operatorname{ord} f).\end{aligned}$$

It follows that $s_0 = \sigma s_0$. Now replace s by the unit $t = s(1 + s_0)^{-1} = 1 + h(1 + s_0)^{-1}$. Since s_0 is invariant under σ, so is $(u_0 - f)\, t$. Moreover, $(u_0 - f)\, t$ has the form

$$u_0 + (\text{terms of degree} \geqslant \operatorname{ord} f).$$

We claim that $u_0 - (u_0 - f)\, t$ is the desired pre-image f' of f: the element f' is invariant in S because both u_0 and $(u_0 - f)\, t$ are invariant. Also $\varphi(f') = f$ since $\varphi(u_0) = f$ and $(u_0 - f)\, t \in \ker \varphi$. Finally, by construction, $\operatorname{ord} f' \geqslant \operatorname{ord} f$ and so the orders must be equal because $\operatorname{ord} x \leqslant \operatorname{ord} \varphi(x)$ for all $x \in S^G$.

Now consider the case of a general $w \in \operatorname{Im} \varphi$ and let $w' \in S^G$ be any element in its inverse image. We need only check that the condition on $\operatorname{ord} w'$ can be met.

Certainly $\operatorname{ord} w' \leqslant \operatorname{ord} w$. If $\operatorname{ord} w' < \operatorname{ord} w$, then all terms of w' of lowest degree are divisible by u_0; any term involving only $u_1, \ldots u_n$ would map to itself under φ and so the order would not increase. Therefore w' has the form

$$w' = u_0 w_0 + \bar{w},$$

where all terms of w_0 have degree (ord w') $-$ 1 and ord $\bar{w} >$ ord w'. Replace u_0 by f' in the expression for w' and call the result w''. The element w'' is again invariant and w'' maps to w since $\varphi(u_0) = \varphi(f') = f$. Furthermore, ord w'' is strictly greater than ord w' because ord $f' >$ ord u_0. Continuing this procedure using w'' in place of w', one will ultimately obtain an element of S^G with order equal to ord w. ∎

Finally, we examine whether the surjectivity of ψ is inherited by φ.

THEOREM 3.13. *Assume that the invariant ring S^G is factorial. Then the map $\varphi\colon S^G \to R^G$ is surjective if and only if the map $R^G \to R$ ramifies only at $\mathfrak{m} \subset R$.*

Proof. Let $\bar{S}$ denote $S^G/\ker\varphi$, which is isomorphic to the image of S^G under φ. Recall that $S^G \to S$ ramifies along the dimension one prime $\mathfrak{p} = (u_0, \ldots, u_{n-1})$ and S^G is singular along its image $\mathfrak{p}' = \mathfrak{p} \cap S^G$ (Proposition 3.5). By Remark 1.9, depth $S^G = 2 + \dim(S/\mathfrak{p}) = 3$ because σ acts linearly on S. Therefore depth $\bar{S} = 2$, since $\ker\varphi$ is principal.

Consider the commutative diagram

$$\begin{array}{ccc} S & \xrightarrow{\psi} & R \\ \uparrow & & \uparrow \\ S^G & \longrightarrow & \bar{S} \end{array}.$$

The map $S^G \to S$ ramifies along the prime $\mathfrak{p}$ and so the induced map $\bar{S} \to R$ ramifies along the image of $\mathfrak{p}$ under ψ, i.e., the ideal $\mathfrak{r} = (f, u_1, \ldots, u_{n-1})$.

We first assume that $R^G \to R$ ramifies only at $\mathfrak{m}$. In this case, the ideal $\mathfrak{r}$ is $\mathfrak{m}$-primary, by Lemma 3.2, and so the map $\bar{S} \to R$ ramifies only in dimension zero. Therefore, in the diagram

$$\begin{tikzcd} & R & \\ \bar{S} \arrow[ur, "\alpha"] \arrow[rr, "\gamma"'] & & R^G \arrow[ul, "\beta"'] \end{tikzcd},$$

the maps α and β are both finite maps of degree p ramified only at $\mathfrak{m}$. Localizing at any non-maximal prime $\mathfrak{q} \subset \bar{S}$, we obtain a corresponding diagram where the localized maps $\alpha_{\mathfrak{q}}$ and $\beta_{\mathfrak{q}}$ are now everywhere unramified. It follows that the third map $\gamma_{\mathfrak{q}}\colon \bar{S}_{\mathfrak{q}} \to R^G_{\mathfrak{q}}$ is also unramified [9; V.3.3], and, having degree one, it is therefore an isomorphism.

Now depth $\bar{S} = 2$ and so this shows that the localization of the map $\bar{S} \to R^G$ is an isomorphism at all primes $\mathfrak{q}$ for which depth $\bar{S}_{\mathfrak{q}} \leqslant 1$. Therefore the map $\bar{S} \to R^G$ is itself an isomorphism [1, Lemma 3], and hence φ is surjective.

We now assume that $R^G \to R$ ramifies in dimension > 0. By Proposition 3.3, the element f contains no u_n^i term and so $f \in \mathfrak{p}$ and $\ker \varphi = (u_0 - f) S \cap S^G$ is contained in $\mathfrak{p}'$. Therefore the restriction of $\mathfrak{p}'$ to $\bar{S}$ is again a non-maximal prime, call it $\bar{\mathfrak{p}}$, and $\bar{S}$ is singular along $\bar{\mathfrak{p}}$. If we localize the map $\operatorname{Spec} S \to \operatorname{Spec} S^G$ at the prime $\mathfrak{p}'$, the result is again a p-cyclic quotient which is now ramified only at the closed point. By Corollary 1.6, the depth of $S^G_{\mathfrak{p}'}$ is 2 and hence depth $\bar{S}_{\bar{\mathfrak{p}}} = 1$. By Serre's criterion, the ring $\bar{S}$ cannot be normal: if ht $\bar{\mathfrak{p}} > 1$, the ring violates the S_2-condition, and if ht $\bar{\mathfrak{p}} = 1$, the fact that $\bar{S}$ is singular along $\bar{\mathfrak{p}}$ violates the R_1-condition. Since R^G is a normal ring, the map φ is not surjective. ∎

4. The Case $n = p - 1$

In order to develop normal forms for the automorphism σ, we next examine which coordinate changes for R preserve σ's partially-linearized form.

Proposition 4.1. *Let $R = k[[u_1, \ldots, u_n]]$ and let σ be an automorphism of R of order p defined by*

$$\begin{aligned} \sigma u_1 &= u_1 + f(u_1, \ldots, u_n), \\ \sigma u_2 &= u_2 + u_1, \\ &\vdots \\ \sigma u_n &= u_n + u_{n-1}, \end{aligned} \tag{4.2}$$

where $f \in R$ has order $\geqslant 2$ and is invariant under σ. Then a change of coordinates $\{u_i\} \mapsto \{\bar{u}_i\}$ preserves the form (4.2) *of σ if and only if*

$$\begin{aligned} \bar{u}_1 &= c_1 u_1 && + c_2 f + (\sigma - 1)^{n-1} h, \\ \bar{u}_2 &= c_2 u_1 + c_1 u_2 && + c_3 f + (\sigma - 1)^{n-2} h, \\ &\vdots \\ \bar{u}_n &= c_n u_1 + c_{n-1} u_2 + \cdots + c_1 u_n + h, \end{aligned} \tag{4.3}$$

where $c_i \in k$, $c_1 \neq 0$, $h \in R$ has order $\geqslant 2$, and $(\sigma - 1)^n h \in R^G$. For this coordinate change, the power series $\bar{f} = \sigma \bar{u}_1 - \bar{u}_1$ is given by

$$\bar{f} = c_1 f + (\sigma - 1)^n h. \tag{4.4}$$

Proof. This is a straightforward exercise in undetermined coefficients and we omit the details. ∎

Using the methods of Section 3 and the above proposition, we now develop a normal form for σ in the case that $n = p - 1$. In this case $(\sigma - 1)^n$ becomes

$$(\sigma - 1)^{p-1} = \sigma^{p-1} + \sigma^{p-2} + \cdots + \sigma + 1,$$

which is the trace operator on R. Therefore the condition $(\sigma - 1)^n h \in R^G$ is trivially satisfied for every $h \in R$ and the expression (4.4) for $\bar{f}$ becomes

$$\bar{f} = c_1 f + \operatorname{tr}(h). \tag{4.5}$$

Thus the power series f can be modified, under a suitable coordinate change, by the trace of any element of R having order at least two.

Now any power series $f \in R^G$ of order at least two determines an automorphism σ via the action (4.2) and the above discussion suggests that two such actions are equivalent exactly when the power series f differ by the trace of an element of order at least two. Therefore the classification of automorphisms reduces to the study of the invariant ring R^G modulo the ideal $\{\operatorname{tr}(h) \mid h \in R,\ \operatorname{ord} h \geqslant 2\}$. To examine the situation for $R = k[[u_1,..., u_{p-1}]]$ we pass to the model $S = k[[u_0, u_1,..., u_{p-1}]]$ on which σ operates by the linear action (3.4).

The invariant ring S^G can be more easily understood if the coordinate system $\{u_i\}$ is replaced by the new coordinates $\{v_i\}$ defined by

$$v_i = \sigma^i u_{p-1}, \qquad i = 0, 1,..., p-1. \tag{4.6}$$

The fact that the v_i determine a coordinate system for S follows from the relation

$$\begin{aligned} u_i = (\sigma - 1)^{p-i-1} u_{p-1} &= \sum_{t=0}^{p-i-1} (-1)^{p-i-1} \binom{p-i-1}{t} \sigma^t u_{p-1} \\ &= \sum (-1)^{p-i-1} \binom{p-i-1}{t} v_t, \end{aligned}$$

and so the coordinates u_i can be recovered as a linear combination of the v_i. In this new system, the automorphism σ acts by

$$\sigma v_i = \sigma^{i+1} u_{p-1} = v_{i+1}, \tag{4.7}$$

and therefore corresponds to a cyclic permutation of the variables v_i. This action by cyclic permutation of the coordinates of $k[[v_0,..., v_{p-1}]]$ is one of the few wild p-cyclic actions that has already been studied (see [8]).

Let M_i denote the module of homogeneous forms of degree i in S. Since σ acts linearly on S, the modules M_i are stable under σ and so can be regarded as G-modules. Let F_m denote the invariant submodule of M_{pm} generated by $(v_0 v_1 \dots v_{p-1})^m$.

LEMMA 4.8. (i) *If $p \nmid i$, then M_i is a free G-module.*

(ii) *If $p \mid i$, let $i = pm$. Then M_{pm}/F_m is a free G-module.*

Proof. The module M_i is generated by monomials of degree i in $v_0, v_1, \dots, v_{p-1}$, and the automorphism σ sends monomials to monomials. We wish to determine how the orbits of monomials partition M_i. If a monomial has fewer than p distinct elements in its orbit, then it is fixed by all of G since the group has prime order. Now σ permutes the variables v_i and so an invariant monomial is symmetric and thus has the form $c(v_0 v_1 \dots v_{p-1})^j$ for some j, where $c \in k$.

If $p \nmid i$, this is impossible and therefore the orbit of each monomial splits off as a free G-module. If $i = pm$, then the elements of F_m are the only fixed monomials; the orbits of the others again determine free G-submodules of M_i. ∎

Lemma 4.8 enables us to understand the structure of S^G as a k-vector space.

PROPOSITION 4.9. *The invariant ring S^G is generated by traces of monomials in S and by powers of $Nv_0 = v_0 v_1 \dots v_{p-1}$.*

Proof. By Lemma 4.8, the orbit of any monomial m which is not a power of Nv_0 has p distinct elements, so any invariant containing m as a term must contain $\sum \sigma^i m = \operatorname{tr} m$. Because this holds for all monomials except $(Nv_0)^j$, any invariant can be expressed as a sum of traces and powers of Nv_0. ∎

We now return to the $\{u_i\}$ coordinate system for S. The element Nv_0 is equal to Nu_{p-1} in the u_i-system, by (4.6). Therefore the above proposition implies

COROLLARY 4.10. *Any $w \in S^G$ can be expressed in the form* $\operatorname{tr} h + q(Nu_{p-1})$, *where q is a power series in Nu_{p-1} and h is an element of S such that* $\operatorname{ord} h \geqslant \operatorname{ord} w$.

Proof. By the proposition, there exists an $h \in S$ and $q \in k[[Nu_{p-1}]]$ such that $w = \operatorname{tr} h + q(Nu_{p-1})$. We can eliminate from h all terms of degree less than $\operatorname{ord} w$ since the trace of these terms vanishes by the homogeneity of the action of σ. ∎

Thus, in the linear model S, the ring of invariants S^G differs from the image of trace only in the existence of power series in Nu_{p-1}. We want to show that this situation is preserved in the passage to the ring R, where the action of σ is nonlinear. We remark that the notation N and tr will now denote the norm and trace for the action of σ on R, not on S.

LEMMA 4.11. *Given any $w \in R^G$ which lies in the image of $\varphi: S^G \to R^G$, there exists an $h \in R$ and $q \in N[[u_{p-1}]]$ such that $w = \operatorname{tr} h + q(Nu_{p-1})$ and* ord $h \geqslant$ ord w.

Proof. This follows from Proposition 3.12 and Corollary 4.10. ∎

THEOREM 4.12. *Let $R = k[[u_1, ..., u_{p-1}]]$ and let σ be an automorphism of R of order p whose linear terms consist of a single Jordan block. Then there is a choice of coordinates for R so that σ has the form*

$$\begin{aligned} \sigma u_1 &= u_1 + (Nu_{p-1})^j, \\ \sigma u_2 &= u_2 + u_1, \\ &\vdots \\ \sigma u_{p-1} &= u_{p-1} + u_{p-2} \end{aligned} \tag{4.13}$$

for some $j \geqslant 1$. Furthermore, the automorphism σ is completely determined by the choice of the integer j. If the map $R^G \to R$ is ramified in dimension greater than zero, then $j = \infty$, i.e., $\sigma u_1 = u_1$ and the action is linear.

Proof. We may assume, by Theorem 2.4, that the action has been brought into partially-linear form with $f = \sigma u_1 - u_1$. The proof is divided into two main steps: we show first that there exists a coordinate change so that f is a power series in Nu_{p-1} and then that coordinates can be chosen so that f is a power of Nu_{p-1} itself.

The first step proceeds by induction. It suffices to show that there exists a converging series of coordinate changes in R under which the terms of f not involving Nu_{p-1} are forced into arbitrarily high degrees. Therefore assume that f is expressed in the form $\operatorname{tr} h + q(Nu_{p-1})$, where $h \in R$ has order $\geqslant n$ and q is a power series in Nu_{p-1}. We show that it is possible to choose coordinates $\bar{u}_i \equiv u_i \pmod{\mathfrak{m}^{n-1}}$ so that the resulting $\bar{f}$ has the form $\bar{f} = \operatorname{tr} \bar{h} + \bar{q}(N\bar{u}_{p-1})$, where ord $\bar{h} \geqslant n+1$ and $\bar{q}$ is a power series in $N\bar{u}_{p-1}$ such that $\bar{q}(N\bar{u}_{p-1}) \equiv q(N\bar{u}_{p-1}) \pmod{\mathfrak{m}^n}$.

Choose new coordinates $\bar{u}_i$ as in Proposition 4.1, letting $c_1 = 1$, $c_i = 0$ for $i > 1$, and setting $\bar{u}_{p-1} = u_{p-1} - h$. Then the corresponding $\bar{f}$ is given by

$$\begin{aligned} \bar{f} = f + \operatorname{tr}(-h) &= \operatorname{tr} h + q(Nu_{p-1}) - \operatorname{tr} h \\ &= q(Nu_{p-1}). \end{aligned}$$

Now $u_{p-1} = \bar{u}_{p-1} + h$, so in the $\bar{u}_i$-system, we have

$$\begin{aligned}\bar{f} &= q(N(\bar{u}_{p-1} + h)) \\ &= q(N\bar{u}_{p-1}) + (\text{terms of degree} \geqslant \text{ord}\, q(Nu_{p-1}) + \text{ord}\, h - 1).\end{aligned}$$

Denote the difference $\bar{f} - q(N\bar{u}_{p-1})$ by δ and note that

$$\text{ord}\,\delta \geqslant \text{ord}\, q(Nu_{p-1}) + \text{ord}\, h - 1 \geqslant n + 1.$$

The power series δ lies in the image of $\varphi\colon S^G \to R^G$ because $\bar{f}$ and $q(N\bar{u}_{p-1})$ do, and so, by Lemma 4.11,

$$\delta = \text{tr}\, \bar{h} + q'(N\bar{u}_{p-1}),$$

for some power series q' in $N\bar{u}_{p-1}$ and some $\bar{h} \in R$ such that ord $\bar{h} \geqslant$ ord δ. Setting $q + q' = \bar{q}$, we obtain

$$\bar{f} = \bar{q}(N\bar{u}_{p-1}) + \text{tr}\, \bar{h},$$

where ord $\bar{h} \geqslant n + 1$. Also $\bar{q}(N\bar{u}_{p-1}) - q(N\bar{u}_{p-1}) = q'(N\bar{u}_{p-1})$ and so has order $\geqslant$ ord $\delta \geqslant n + 1$. Therefore this coordinate change satisfies the conditions mentioned above, thus completing step one.

Assume now that $f = q(Nu_{p-1})$ for some power series q and write f as

$$f = (Nu_{p-1})^j (c_0 + c_1(Nu_{p-1}) + c_2(Nu_{p-1})^2 + \cdots),$$

for some $j > 0$, where $c_i \in k$ and $c_0 \neq 0$. Set $c = c_0 + c_1(Nu_{p-1}) + \cdots$, which is a unit in R^G.

Let $\alpha \in R^G$ be a solution to the equation

$$\alpha^{pj-1} = c.$$

Such a solution exists because R^G is complete and $pj - 1$ is prime to p. Now consider the map $u_i \mapsto \bar{u}_i$ where $\bar{u}_i = \alpha u_i$. This is an invertible transformation since α is a unit and so defines a coordinate change in R. Under this change we have

$$\begin{aligned}\bar{f} = \alpha f &= \alpha c(Nu_{p-1})^j \\ &= \alpha^{pj}(Nu_{p-1})^j \\ &= N(\alpha u_{p-1})^j \\ &= N(\bar{u}_{p-1})^j.\end{aligned}$$

Hence $\bar{f}$ has the required form.

Given any integer $j \geqslant 1$, the element Nu_{p-1}, and hence the action of σ, is completely determined by the set of Eqs. (4.13). To establish this, consider the identity

$$Nu_{p-1} = \prod_{i=0}^{p-1} \sigma^i u_{p-1}.$$

By expanding $\sigma^i u_{p-1}$ in terms of the action (4.13), we obtain a polynomial expression for Nu_{p-1} in terms of $u_1,..., u_{p-1}$, and $(Nu_{p-1})^j$. The expression for Nu_{p-1} can then be substituted into $(Nu_{p-1})^j$ in this polynomial and, by repeating this process, we can eliminate Nu_{p-1} recursively, resulting in a formula for Nu_{p-1} in terms of $u_1,..., u_{p-1}$ alone. Thus Nu_{p-1} depends only on the choice of j.

Finally, if the map $R^G \to R$ ramifies in dimension >0 then, by Proposition 3.3, the power series f contains no term of the form u_{p-1}^i. Since $Nu_{p-1} = u_{p-1}^p + ...$, this implies that $f = 0$ and the resulting action is linear. ∎

Thus, by a suitable change of coordinates the action of σ can be brought into a particularly simple form. In the case $p = 3$, the invariant ring R^G is Cohen–Macaulay and an explicit equation for the quotient-singularity resulting from the action (4.13) can be computed (see Corollary 5.15). However, even when $p = 5$, the ring structure of R^G is not known.

5. The Case $n = 2$

We next apply the methods of Section 3 to the case of surface singularities. Therefore let $R = k[[u_1, u_2]]$ and let σ be the p-cyclic automorphism of R defined by

$$\begin{aligned} \sigma u_1 &= u_1 + f, \\ \sigma u_2 &= u_2 + u_1, \end{aligned} \tag{5.1}$$

where $f \in R^G$ has order $\geqslant 2$. The linear model S for this action is $k[[u_0, u_1, u_2]]$ with homogeneous action given by

$$\begin{aligned} \sigma u_0 &= u_0, \\ \sigma u_1 &= u_1 + u_0, \\ \sigma u_2 &= u_2 + u_1. \end{aligned} \tag{5.2}$$

Here $\dim R^G = 2 = \operatorname{depth} R^G$ (by Proposition 1.4) and $\dim S^G = 3 =$

depth S^G (by Remark 1.9) and so both invariant rings are Cohen–Macaulay. In this case it is possible to write down equations defining these rings explicitly.

We begin by examining the linear model S. The invariant ring S^G contains the elements u_0, Nu_1, and Nu_2. Denoting Nu_1 by x and Nu_2 by y, we have

$$\begin{aligned} x &= \prod \sigma^i u_1 = \prod_{m=0}^{p-1} (u_1 + mu_0) \\ &= u_1^p - u_0^{p-1} u_1, \\ y &= \prod \sigma^i u_2 = \prod_{m=0}^{p-1} (u_2 + mu_1 + \tbinom{m}{2} u_0) \\ &= u_2^p - u_1^{p-1} u_2 + (\text{terms divisible by } u_0). \end{aligned} \tag{5.3}$$

Let S' denote the subring of S^G generated by u_0, x, and y.

LEMMA 5.4. *The rings S and S^G are free S'-modules of ranks p^2 and p, respectively.*

Proof. The elements u_0, x, and y form a system of parameters in S; hence S is a finite extension of S'. The ring S is regular, therefore Cohen–Macaulay, and so the extension is free [13, IV, Proposition 22]. A basis is given by the p^2 elements $\{u_1^i u_2^j\}$, $0 \leqslant i, j \leqslant p-1$. Now the extension $S^G \to S$ is finite of rank p, so S^G has rank p over S'. Again the extension is free because S^G is Cohen–Macaulay. ∎

The element

$$z = u_1^2 - u_0 u_1 - 2u_0 u_2 \tag{5.5}$$

is also invariant under σ and z is not contained in S' because its degree in u_0, u_1, u_2 is two. We claim that z generates the extension S^G over S'.

LEMMA 5.6. *The invariant z satisfies the relation $\mathscr{R} = 0$ over the ring S', where*

$$\mathscr{R} = z^p + \sum_{n=2}^{(p+1)/2} (-1)^n c_n u_0^{2p-2n} z^n + 2u_0^p y - x^2 \tag{5.7}$$

and the coefficients c_n are the Catalan numbers, $c_n = (2n-2)!/n!(n-1)!$.

Proof. The following argument, which replaces our overlong verification, is due to Ira Gessel. The relation $\mathscr{R}$ is homogeneous of degree $2p$ in u_0, u_1, and u_2 and so, for simplicity, we verify the relation in the inhomogeneous form obtained by setting $u_0 = 1$. Therefore, replace the elements x, y, and z by their inhomogeneous forms

$$x = \prod_{m=0}^{p-1} (u_1 + m) = u_1^p - u_1,$$

$$y = \prod_{m=0}^{p-1} \left(u_2 + mu_1 + \tbinom{m}{2}\right),$$

$$z = u_1^2 - u_1 - 2u_2.$$

The numbers c_n can be expressed in terms of binomial coefficients:

$$\binom{\frac{1}{2}}{n} = \frac{(\frac{1}{2})(-\frac{1}{2}) \cdots (-(2n-3)/2)}{n!} \qquad \text{for } n \geqslant 1$$

$$= \frac{(-1)^{n-1}}{2^n} \cdot \frac{1 \cdot 3 \cdots (2n-3)}{n!} \cdot \frac{2 \cdot 4 \cdots (2n-2)}{2 \cdot 4 \cdots (2n-2)}$$

$$= \frac{(-1)^{n-1}}{2^{2n-1}} \frac{(2n-2)!}{n!(n-1)!}$$

$$= \frac{(-1)^{n-1}}{2^{2n-1}} \cdot c_n.$$

Therefore we obtain

$$\sum_{n=2}^{(p+1)/2} (-1)^n c_n z^n = -\sum_{n=2}^{(p+1)/2} 2^{2n-1} \binom{\frac{1}{2}}{n} z^n$$

$$= -\frac{1}{2} \sum_{n=2}^{(p+1)/2} \binom{\frac{1}{2}}{n} (4z)^n$$

$$= -\frac{1}{2} \left((1+4z)^{(p+1)/2} - 1 - \left(\frac{p+1}{2}\right)(4z)\right)$$

$$= -\tfrac{1}{2}((1+4z)^{(p+1)/2} - 1 - 2z).$$

In order to develop a suitable expansion for the product defining y we note

$$\prod_{m=0}^{p-1} (\alpha + (m+\beta)^2) = \alpha(\alpha^{(p-1)/2} - (-1)^{(p-1/2)})^2 - (\beta^p - \beta)^2.$$

To prove this it suffices to check that the right-hand side vanishes when $\alpha = -(m+\beta)^2$ for $m = 0, \ldots, p-1$. This is straightforward and we omit the details.

Now setting

$$\begin{aligned}\alpha &= 2u_2 - (u_1 - \tfrac{1}{2})^2 \\ &= - z - \tfrac{1}{4}\end{aligned}$$

and setting $\beta = u_1 - \frac{1}{2}$, we have

$$\begin{aligned}\alpha + (m+\beta)^2 &= 2u_2 - (u_1 - \tfrac{1}{2})^2 + (m + u_1 - \tfrac{1}{2})^2 \\ &= 2(u_2 + mu_1 + \tbinom{m}{2}).\end{aligned}$$

Therefore

$$\begin{aligned}2y &= 2^p \prod_{m=0}^{p-1} (u_2 + mu_1 + \tbinom{m}{2}) \\ &= \prod_{m=0}^{p-1} (\alpha + (m+\beta)^2) \\ &= (-z - \tfrac{1}{4})((-z-\tfrac{1}{4})^{(p-1)/2} - (-1)^{(p-1)/2})^2 - ((u_1 - \tfrac{1}{2})^p - (u_1 - \tfrac{1}{2}))^2 \\ &= - z^p + \tfrac{1}{2}((1+4z)^{(p+1)/2} - 1 - 2z) + (u_1^p - u_1)^2 \\ &= - z^p + x^2 - \sum (-1)^n c_n z^n. \quad \blacksquare\end{aligned}$$

PROPOSITION 5.8. *The invariant ring S^G is defined by*

$$S^G = S'[z]/(\mathscr{R}),$$

where $\mathscr{R}$ is the relation (5.7).

Proof. Clearly, we have the inclusions

$$S' \subsetneq S'[z]/(\mathscr{R}) \subset S^G.$$

Both S^G and $S'[z]/(\mathscr{R})$ are degree p extensions of S' and the relation $\mathscr{R}$ is irreducible. Therefore to show $S'[z]/(\mathscr{R}) = S^G$, it suffices to show that the ring $S'[z]/(\mathscr{R})$ is normal.

Consider the partial derivatives

$$\frac{\partial \mathscr{R}}{\partial x} = - 2x,$$

$$\frac{\partial \mathscr{R}}{\partial y} = 2u_0^p.$$

These partials vanish simultaneously only along the codimension two locus $\{x = u_0 = 0\}$. Thus $S'[z]/(\mathscr{R})$ is non-singular in codimension one and, being a hypersurface, it is therefore normal. ∎

Now consider the situation for the ring R. The ring of invariants R^G contains Nu_1 and Nu_2, where the norms are now computed with respect to the inhomogeneous action of σ on R. We continue to denote these norms by x and y; they are the images of the above x and y under the map $\varphi: S^G \to R^G$. Note that now

$$\begin{aligned} x &= u_1^p - f^{p-1}u_1 = u_1^p + (\text{terms of degree } > p), \\ y &= u_2^p - u_1^{p-1}u_2 + (\text{terms of degree } > p) \end{aligned} \tag{5.9}$$

and therefore x and y alone form a system of parameters for R.

Consequently, we obtain the following analogue of Lemma 5.4:

LEMMA 5.10. *The rings R and R^G are free $k[[x, y]]$-modules of ranks p^2 and p, respectively.*

Now suppose that the map $R^G \to R$ ramifies only at the maximal ideal $\mathfrak{m} \subset R$ so that R^G has an isolated singularity. If Conjecture 3.10 is true, the map $\varphi: S^G \to R^G$ is surjective, by Theorem 3.13, and so R^G is generated by the images of x, y, z, and u_0 under φ. Denote the element $\varphi(z)$ again by z.

PROPOSITION 5.11. *If the map $\varphi: S^G \to R^G$ is surjective, then R^G is generated over $k[[x, y]]$ by the single invariant z.*

Proof. Any $w \in R^G$ can be expressed as a power series in x, y, z, and $f = \varphi(u_0)$. It suffices to show that all terms involving f can be forced into arbitrarily high degrees.

By Proposition 3.12 there exists an element $w' \in S^G$, such that $\varphi(w') = w$ and $\operatorname{ord} w' = \operatorname{ord} w$. Write w' in the form $r + u_0 s$, where r depends only on x, y, and z. Now

$$w = \varphi(r + u_0 s) = \varphi(r) + f \cdot \varphi(s).$$

Therefore $\operatorname{ord} w = \operatorname{ord}(\varphi(r))$, whereas $\operatorname{ord}(f \cdot \varphi(s)) > \operatorname{ord}(u_0 s) \geqslant \operatorname{ord} w$. Thus the terms in w involving f lie in degrees strictly greater than $\operatorname{ord} w$. Set $w_1 = f \cdot \varphi(s)$ and repeat the argument using w_1 in place of w. By continuing in this manner we conclude that a representation for w can be found in which terms involving f have arbitrarily high degree. ∎

The elements x, y, z, and f satisfy the relation

$$\mathscr{R}' = z^p + \sum_{n=2}^{(p+1)/2} (-1)^n c_n f^{2p-2n} z^n + 2f^p y - x^2 = 0 \tag{5.12}$$

in R^G, corresponding to the relation $\mathscr{R}$ satisfied by x, y, z, and u_0 in S^G. If the map φ is surjective, then the preceding proposition implies that f lies in $k[[x, y, z]]$ and hence that $\mathscr{R}'$ defines a relation among x, y, and z alone. In fact, we now show that even without the assumption of surjectivity, the hypothesis that f lies in $k[[x, y, z]]$ is sufficient to prove that $R^G = k[[x, y, z]]/(\mathscr{R}')$.

LEMMA 5.13. *The map $R^G \to R$ ramifies only at the maximal ideal $\mathfrak{m} \subset R$ if and only if f is relatively prime to x and z.*

Proof. By Proposition 3.3, the map is unramified away from $\mathfrak{m}$ if and only if f contains a term of the form u_2^i, for some i. Now $x = u_1^p - f^{p-1}u_1$ and $z = u_1^2 - fu_1 - 2fu_2$, so f is relatively prime to x and z exactly when it is not divisible by u_1. Since the only variables in R are u_1 and u_2, this requires that f contain a pure u_2-term. ∎

THEOREM 5.14. *If $f \in k[[x, y, z]]$ and the map $R^G \to R$ ramifies only at $\mathfrak{m}$, then the ring of invariants R^G is equal to*

$$k[[x, y, z]]/(\mathscr{R}')$$

where $\mathscr{R}'$ is the relation (5.12).

Proof. As in Proposition 5.8, it suffices to show that the relation $\mathscr{R}'$ defines a normal quotient of $k[[x, y, z]]$. Consider the partial derivatives

$$\frac{\partial \mathscr{R}'}{\partial x} = -2x + \sum_{n=2}^{(p+1)/2} (-2n)\, c_n f^{2p-2n-1} z^n \left(\frac{\partial f}{\partial x}\right),$$

$$\frac{\partial \mathscr{R}'}{\partial y} = 2f^p + \sum_{n=2}^{(p+1)/2} (-2n)\, c_n f^{2p-2n-1} z^n \left(\frac{\partial f}{\partial y}\right),$$

$$\frac{\partial \mathscr{R}'}{\partial z} = \sum_{n=2}^{(p+1)/2} \left[(-2n)\, c_n f^{2p-2n-1} z^n \left(\frac{\partial f}{\partial z}\right) + n c_n f^{2p-2n} z^{n-1}\right]$$

$$= f^{p-2} z(2c_2 f^{p-2} + \text{terms divisible by } z).$$

There are three cases to examine:

(i) If $f = 0$, then $\partial \mathscr{R}'/\partial y = \partial \mathscr{R}'/\partial z = 0$ and $\partial \mathscr{R}'/\partial x = -2x$. The elements f and x are relatively prime, by Lemma 5.13, and so vanish simultaneously only at the maximal ideal $\mathfrak{m}'$ of $k[[x, y, z]]/(\mathscr{R}')$.

(ii) If $z = 0$, then $\partial \mathscr{R}'/\partial x = -2x$ and $\partial \mathscr{R}'/\partial y = 2f^p$ and again these simultaneously vanish only at $\mathfrak{m}'$.

(iii) The only other possibility for which $\partial \mathscr{R}'/\partial z = 0$ is that $2c_2 f^{p-2}$ is contained in the ideal generated by z. But f and z are relatively prime and $c_2 \neq 0$, so again this happens only at $\mathfrak{m}'$.

Therefore $k[[x, y, z]]/(\mathscr{R}')$ is singular only at the maximal ideal. Since the ring is non-singular in codimension one and defines a hypersurface, it is normal. ∎

As in the previous section, it would be nice to know how much the choice of f can be normalized under a suitable coordinate change. By Proposition 4.1, f can be altered by an element of the form $(\sigma - 1)^2 h$ in R^G, provided $h \in R$ has order at least two. It is easy to check that x has this form and can therefore be eliminated by arguing as in the proof of Theorem 4.12, while y does not. We have not yet determined the situation for z.

However, in the special case that $p = 3$, the dimensions 2 and $p - 1$ coincide so that the results of Sections 4 and 5 can be combined to obtain

COROLLARY 5.15. *Let $R = k[[u_1, u_2]]$, where* char $k = 3$, *and let σ be any automorphism of R of order* 3 *whose linear terms consist of a single Jordan block. If the map $R^G \to R$ ramifies only at the maximal ideal of R, then*

$$R^G = k[[x, y, z]]/(z^3 + y^{2j} z^2 - y^{3j+1} - x^2) \tag{4.16}$$

for some $j > 0$. If the map ramifies in dimension one, then R^G is regular.

Proof. By Theorem 4.12, there exists a choice of coordinates for R so that σ has the form

$$\sigma u_1 = u_1 + y^j,$$
$$\sigma u_2 = u_2 + u_1$$

for some $j > 0$, where $y = N u_2$. If the map $R^G \to R$ ramifies only in dimension zero, then Theorem 5.14 gives the desired form for R^G. If the map is ramified in dimension one, then $j = \infty$ and σ is given by the linear action

$$\sigma u_1 = u_1,$$
$$\sigma u_2 = u_2 + u_1.$$

The elements u_1 and $N u_2 = u_2^p - u_1^{p-1} u_2$ are invariant under this action and it is easy to check that they are algebraically independent and generate the invariant ring. Thus R^G is regular. ∎

It is interesting to note that if $j = 1$, then the resulting singularity (4.16) is a rational double point of type E_6. However, in the range $1 < j < \infty$, the singularities, though Cohen–Macaulay, are no longer rational.

6. Remarks on Extending the One-Block Forms

Finally we illustrate how the basic one-block actions of the preceding sections may be generalized to several block forms. Given any p-cyclic automophism σ of the ring $R = k[[u_1, u_2, ..., u_n]]$, the action of σ can be brought into the partially linearized form (2.5). Following the methods of Section 2, a linear model can then be constructed where one new variable is added for each nonlinear term appearing in the extended form (2.7) for σ. However, if the number of new variables is greater than one, the methods of Section 3 must be modified: the invariant ring R^G no longer can be realized as a simple hypersurface slice of S^G and the coordinate changes required to bring each of the higher order terms into canonical form must be compatibly chosen.

Consider, for example, the case that $R = k[[u_{1,1}, ..., u_{1,p-1}; ...; u_{n,1}, ..., u_{n,p-1}]]$ and σ is a p-cyclic automorphism of R whose linear part consists of n Jordan blocks, each of the maximal nonlinear dimension $p-1$. By Theorem 2.4, there exists a choice of coordinates so that the action of σ within each Jordan block has the form

$$\begin{aligned} \sigma u_{i,1} &= u_{i,1} + f_i(u_{1,1}, ..., u_{n,p-1}), \\ \sigma u_{i,2} &= u_{i,2} + u_{i,1}, \\ &\vdots \\ \sigma u_{i,p-1} &= u_{i,p-1} + u_{i,p-2}, \end{aligned} \tag{6.1}$$

for $i = 1, ..., n$, where $f_i \in R$ has order $\geqslant 2$ and is invariant under σ. Note that each f_i may involve all of the $u_{j,k}$'s, not only those within its block. In the one-block case, Theorem 4.12 shows that it is possible to choose coordinates so that the single higher-order term f is a power of Nu_{p-1}. However, in a several-block action, there is a possibility of interplay between the higher-order terms of different blocks. We therefore conjecture that Theorem 4.12 has the following generalization:

Conjecture 6.2. For R and σ as above, there exists a choice of coordinates so that $f_i = q_i(Nu_{1,p-1}, ..., Nu_{n,p-1})$, where q_i is a power series in the norms of $u_{j,p-1}$ for $j = 1, ..., n$. If the map $R^G \to R$ ramifies only at the maximal ideal, then the ideal $(f_1, ..., f_n)$ is primary to $(u_{1,p-1}, ..., u_{n,p-1})$.

In the case $n = p = 2$, this result has been established by Artin [2]. In characteristic two, the maximal size for a nonlinear Jordan block is one, so that σ has the form

$$\begin{aligned} \sigma u_1 &= u_1 + f_1, \\ \sigma u_2 &= u_2 + f_2, \end{aligned}$$

where $f_i = q_i(Nu_1, Nu_2)$. If the action is free except at the closed point, then (f_1, f_2) is primary to the maximal ideal $\mathfrak{m} = (u_1, u_2)$ and hence f_1 and f_2 are relatively prime. In this case the resulting invariant ring is generated by the three elements $x = Nu_1$, $y = Nu_2$, and $z = u_1 f_2 + u_2 f_1$, subject to the single relation

$$z^2 + f_1 f_2 z + f_1^2 y + f_2^2 x = 0.$$

This action is one of the basic forms arising in the study of rational double points in characteristic two. For example, if $f_1 = x$ and $f_2 = y$, the resulting quotient-singularity is defined by the equation

$$z^2 + xyz + x^2 y + y^2 x = 0,$$

which is a double point of type D_4.

Further examples of wild group actions can be found in [11] where the actions generating the rational double points in characteristic p are explicitly computed.

Acknowledgment

The main results of this paper form a part of the author's doctoral dissertation. I would like to thank my advisor, Michael Artin, for all the advice and encouragement he provided during this work.

References

1. A. Altman and S. L. Kleiman, On the purity of the branch locus, *Compos. Math.* **23** (1971), 461–465.
2. M. Artin, Wildly ramified $Z/2$ actions in dimension two, *Proc. Amer. Math. Soc.* **52** (1975), 60–64.
3. M. Artin, "Coverings of the rational double points in characteristic p," *in* "Complex Analysis and Algebraic Geometry," Cambridge Univ. Press, London/New York, 1977.
4. E. Brieskorn, Rationale Singularitäten komplexer Flächen, *Invent. Math.* **4** (1968), 336–358.
5. H. Cartan, Quotient d'un espace analytique par un groupe d'automorphismes, *in* "Algebraic Geometry and Topology," Princeton Univ. Press, Princeton, N.J., 1957.
6. G. Ellingsrud and T. Skjelbred, Profondeur d'anneaux d'invariants en caractéristique p, *Compt. Rend.* **286** Ser. A (1978), 321–322.
7. J. Fogarty, On the depths of local rings of invariants of cyclic groups, *Proc. Amer. Math. Soc.* **83** (1981), 448–452.
8. R. M. Fossum and P. A. Griffith, Complete local factorial rings which are not Cohen-Macaulay in characteristic p, *Ann. Sci. École Norm. Sup.* **8** (1975), 189–199.
9. A. Grothendieck, "Revêtements Étales et Groupe Fondamental (SGA 1), Séminaire de Géométrie Algébrique du Bois Marie 1960/61," Lecture Notes in Mathematics No. 224, Springer-Verlag, Berlin/New York, 1971.
10. H. Matsumura, "Commutative Algebra," Benjamin, New York, 1970.

11. B. R. PESKIN, "Quotient-singularities in characteristic p," Ph.D. Thesis, M.I.T., 1980.
12. P. SAMUEL, Classes de diviseurs et dérivées logarithmiques, *Topology* **3** (1964), 81–96.
13. J.-P. SERRE, "Algèbre Locale—Multiplicités," Lecture Notes in Mathematics No. 11, Springer-Verlag, Berlin/New York, 1965.
14. O. ZARISKI, On the purity of the branch locus of algebraic functions, *Proc. Nat. Acad. Sci. USA* **44** (1958), 791–796.